通信情報保護學會誌
第1卷, 第2號, 1991. 8

UNIX 시스템 보안 가이드

임 채 호*

1. 개 요

엔지니어링 워크스테이션이 PC 만큼 널리 쓰여지고 있고, 또 미국방성 네트워크 구조인 TCP/IP 프로토콜에 의한 LAN 및 각종 대형의 전산망이 국내에서도 점차 정착됨에 따라 AT&T UNIX에서 비롯된 System V UNIX, Berkeley 대학의 BSD UNIX 들이 많이 이용되고 있다.

하지만 UNIX 운영체제는 애초에 보안성을 염두에 두고 개발된것이 아니고 연구실 환경에서 개방된 공동연구 환경에 알맞는 시스템이라 볼 수 있다. 그런데 1980년대부터 UNIX 시스템은 각 연구소 대학 뿐 아니라 상업용에 이르기까지 다양한 하드웨어에 이식되어 네트워크에 사용자에 개방되어지고 있는 추세이며, UNIX로부터 운영체제의 국제표준이 이루어지고 있다. 이러한 급격한 발전과 UNIX의 새로운 유틸리티, 특징들이 더해지고 있지만, 사용자의 보안문제를 완벽하게 해결해 주지 못하고 있는 실정이라고 하겠다.

보안이 문제가 되는 UNIX의 기능들은 대부분 네트워크에 관련한 것이 대부분으로서, 열거하자면,

- Remote Login,
- Remote Command Execution,
- Network File System,
- Diskless Workstation,
- Electronic Mail

등이다. 물론 UNIX의 다른 기능들도 세심한 주의로서 관리하지 않으면 항상 보안에 문제가 생길 여지가 있으므로 UNIX 보안은 대우 중요한 주제임에 틀림없다. 여기서 잠깐 UNIX 환경에서의 보안사고의 대표적인 사례를 잠깐 살펴보면,

• Internet Worm :

UNIX 시스템의 보안 문제를 가장 심각하게 드러낸 사고의 하나로서, 1988년 11월 2일, Robert Tappan Morris라는 Cornell 대학의 대학원생이 만든 프로그램이 한밤중에 Internet에 복제되어 퍼져, Berkeley 대학, NASA 등 주요 Internet 기관의 호스트 수천대가 감염되었는데, 전자우편전송 프로그램인 SMTP의 DEBUG, Finger, Password 공격, Rlogin 등을 이용한 Worm은 시스템의 과부하 및 전송매체의 폐닉으로 일시에 장애를 유발하였다. Worm은 SUN 워크스테이션, VAX기종의 BSD 계열 UNIX 시스템을 감염시켰느데, 사건발생 1주일만에 Worm을 방지가능한 BSD Source를 네트워크를 통하여 배포하고 있다. Morris는 사건 후 연방수

* 정회원, 한국과학기술연구원 시스템공학 연구소

사국에 의해 정부전산자원 오용 혐의로 기소되어 1만불의 벌금과 사회봉사 판결을 받았고, Cornell 대학에서 영구 추방되었다. 이 Worm 사건에서 주목할 사항은 NASA의 신속한 경보발송과 긴급 대책회의를 열고 단 1주일만에 방지가능한 BSD Source를 발표하였다는 점이다.

• 군사스파이사건

1986년 8월 Berkeley 대학의 시스템에 한 침입자가 있었는데, 시스템 관리자, Clifford Stoll은 시스템을 막는 대신 그 침입자를 계속 모니터 하기로 하고 추적해본 결과, 세계적으로 400대가 넘는 시스템을 공격하여 그 중 30대에 성공적으로 침입하는 것을 발견했을 뿐 아니라, 우주왕복선, SDI 등 군사적인 정보를 빼낸다는 사실을 확인하였다. 1년에 걸친 추적끝에, 서독 거주의 5명을 군사기밀을 KGB에 팔아 넘긴 혐의로 기소하였는데, 그 중 1명은 의문의 변사체로 발견되기까지 하였다.

그밖에도 최근에는 여러 보안문제가 발생되었는데, NASA의 SPAN, Mitre Corp, 의 IBM 기종에서 발생된 "Christmas Virus", DECNET의 Worm, 미국 은행네트워크에서 발생된 보안문제 등이 있다. 열거된 것들은 빙산의 일각일 뿐 무수한 보안문제가 있음을 시스템 관리자 및 사용자는 명심해야 할 것이다.

여기에서는 미국 스탠포드 연구소(SRI)에서 1990년에 발표된 "Impoving The Security of Your UNIX System" 자료와, 한국과학기술연구원 시스템 공학 연구소에서 1991년 2월에 발간한 보고서, "R&D 네트워크에서의 컴퓨터 바이러스 및 시스템 보호대책에 관한 연구"를 참고로 주로 SUN 시스템 즉, BSD 계열의 UNIX 시스템 보안에 대한 가이드를 정리 소개하고자 한다.

2. UNIX 보안 향상방법

2.1 사용자 계정

2.1.1 패스워드(passwords)

시스템 공격자는 대부분 사용자의 패스워드를 교묘한 방법으로 얻고는 시스템을 공격하게 되는데, 만약 관리자(root) 패스워드를 얻게된다면 치명적인 보안문제를 야기하게 된다. UNIX의 password 프로그램은 최소한 4개 혹은 5개 이상의 문자를 원하지만 사용자가 이하갯수의 패스워드를 고집하면 허용할 수 있도록 되어 있다. 즉 3번 이상 입력하게 되면 허용하는 것이다.

미국에서의 한 조사에 의하면, 3,289개의 사용자 패스워드를 수집하고 통계를 뽑은 결과 16%가 3자리 이하이면, 86%가 쉽게 연상가능한 것이라는 놀라운 사실이다. 가령 계정을 그대로 패스워드로 쓰거나, 역순 혹은 2가지를 섞은 것이다. 혹은 많은 패스워드가 알려진 여자의 이름, 약자 등이라는 것도 알게 되었는데, 공격자는 어느 한 시스템에서 8내지 20%의 사용자 계정을 알아낼 수 있다고 하며, 어쨌든 50%의 패스워드는 2, 3일의 노력으로 알아내 수 있다고 한다.

이제 패스워드를 선택하는 지침을 보게되면,

- 로그인 이름을 쓰지 말것,
- 사용자 자신의 이름을 쓰지 말것,
- 아이들이나 이성파트너의 이름을 쓰지 말것,
- 자신의 신변정보를 쓰지 말것,
- 패스워드를 모두 숫자로 하거나, 동일한 문자를 반복하지 말것,
- 사전이나 시스템 워드에서 따오지 말것,
- 6개 이상의 문자를 쓸것,
- 대소문자를 섞어 쓸것,
- 가능한 특수문자나 숫자를 섞을것,
- 적어둘 필요없는 기억하기 쉬운 것을 쓸것,
- 키보드를 보지않고 쉽게 타이핑할 수 있는것을 쓸것.

으로서 만약 이 기준만을 생각한다면, 패스워드를 선택하기가 매우 어려울 것이다. 그렇다면, 다음의 패스워드 선택 요령을 보기로 하자.

- 알려진 노래나 시의 한줄에서 첫문자를 선택
  * 영시나 영어권 노래를 모른다면 국내것을 로마자 이니셜을 선택할 수 있을 것이다.

- 의성어를 섞어 선택하면, 비상식적 단어를 만들 수 있다.
- 2개의 단어를 ":", "?" 등을 끼워 선택,(예, book ? sky)
- 만약 한글 키보드가 있다면, 한글로 영문을 선택하는 것도 방법,

이렇게 보안성이 높은 패스워드 선택요령만으로도 부족하여 패스워드 정책을 수립해두는 것이 좋다. 이것은 각 기관마다 나름대로의 정책을 수립할 수 있겠지만,

- 사용자에게 패스워드는 자신의 마음속에서만 기억하도록 주지시키고,
- 사용자에게 자신의 패스워드를 타인에게 대여할 수 없음을 주지시키고,
- 사용자에게 패스워드를 가끔 변경하도록 주지시켜야

하는 것이 무엇보다 주용하다. 이렇게 지침을 마련해 두어도 사실은 사용자가 잘 따르지 않으므로 관리자는 마치 공격자처럼 사용자의 패스워드를 깨도록 시도하는 프로그램을 주기적으로 수행시켜야 한다. 이런 프로그램은 Anonymous FTP로 소스를 가져다 쓸 수 있다.

2.1.2 계정의 만기

여러기관의 호스트, 특히 서버기종들은 계정을 많이 가지고 있어서, 사용하지 않는 사용자 계정이 많기 마련이다. 이렇게 사용되지 않는 계정들은 보안의 헛점이 되고 특히 아무도 사용하지 않기 때문에 그 보안의 문제를 인식하기도 어렵게 된다. 이것을 방지하는 가장 손쉬운 방법은 각 계정마다 만기일을 설정해 두는 것이다. 흔히 각 계정은 1년의 기한을 두는 것이 좋으며, /etc/passwd 화일의 사용자이름 필드에 만기일을 기입해 두고 주기적으로 Shell Script를 수행하는 데, 매달 1회 만기계정의 사용자의 퇴직, 졸업 등의 상황을 체크해 보는 것이 좋다.

2.1.3 손님계정(guest, sonnim, general 등)

아직도 국내에서는 sonnim이나, guest 등의 계정을 유지하는 호스트가 꽤 있는 것으로 여겨지는데, 이것은 마찬가지로 보안의 헛점이 된다. 이것이 정 필요하다면, 필요에 따라 만들고 지우는 방법을 택해야 할 것이다.

2.1.4 패스워드 없는 계정

그리고 많은 호스트가 패스워드 없이 단순한 명령을 수행하는 계정들을 사용하고 있다. 예를 들어 who, date, lpq, 그리고 중계하는 호스트 이름을 사용하여 telnet 명령어를 수행하고 사용자 id를 0로 둠으로서, 시스템 관리자(root)급의 수행을 허용하는 데, 이는 시스템 공격자가 프로그램을 옮기는 좋은 도구를 제공하는 결과를 초래하게 된다. 기본적으로 UNIX에는 패스워드 없는 계정을 만들어서는 안된다.

2.1.5 그룹계정(Group Account)

여러명의 사용자가 공동으로 사용하는 계정을 만들 수 있다. 이것도 하나의 보안에 문제를 야기할 수 있는데, 여러명의 가입자가 패스워드를 공유하는 문제가 벌써 보안지침에 위배되는 것이다. 하지만 공동연구 등 정보의 공유가 필요한 경우는 그룹계정보다 /etc/group에 각각의 사용자를 등록하여 사용하면 된다./etc/group 은,

groupname : passwd : groupid : user1, user2, user3, …

위의 엔트리로 구성되는 데, groupname은 로그인 이름과 같은 그룹이름이며, passwd는 사용되지 않으므로 *만 입력하고, groupid는 보통 10부터 65535까지의 숫자를 이용하면 된다. 그리고 그 그룹에 해당하는 사용자를 입력하는 데, 각각의 사용자는 자신의 계정과 패스워드를 따로 가지게 되지만 동일 그룹에 의해 화일과 디렉토리를 공유할 수 있어서, 시스템의 보안을 향상할 수 있다.

예를 들어/etc/group에 다음의 엔트리가 있다면,

staff : * : 30 : ohbyeon, chlim, khcho, schan, sjahn

chgrp와 chmod 명령을 통하여 program을 공유할 수 있다.

```
% chgrp staff ~ chlim/program
% chmod -R g+rw ~ chlim/program
```

2.1.6 Yellow Pages

SUN의 Yellow Page 시스템은 여러 호스트가 네트워크를 통하여 패스워드 화일과 그룹화일 등을 공유할 수 있도록 하는 기능이다. 이것은 Client 시스템의 passwd와 group 화일의 각 엔트리에 +를 입력해두면 이 정보들은 Master 시스템에서 정보를 가져오게 된다. 일반적으로 Yellow Page는 보안성이 있는 것으로 여겨지지만, 다음과 같이 passwd와 group 화일에서,

```
+ : : 0 : 0 : : :   # passwd 화일
+ :                 # group 화일
```

에서 "+"를 잃어버릴 경우 패스워드 없는 빈 계정에 0 사용자 id의 관리자 권한을 가지게 되어 시스템이 그냥 개방되는 결과를 초래하게 된다. Yellow Page는 매우 유용한 유틸리티이니 만큼 조심스럽게 사용해야 할 것이다.

2.2 네트워크의 보안

2.2.1 개요

UNIX를 비롯한 여러기종들이 이기종간의 인터네트워킹을 미국방성 망구조인 TCP/IP 프로토콜을 이용하여 각자의 기관 LAN과, 지역, 국가의 WAN에 연결하고 뿐만 아니라 전세적으로 연결을 시도하는 추세가 이루어짐에 따라, 각각의 호스트는 세계적으로 개방되어 언제라도 세계의 어느 누구라도 액세스 가능하게 되었는데, 이는 사용자에게 네트워크의 편리함을 주지만 시스템의 보안에 문제를 야기할 가능성이 높아졌으므로 시스템을 외부의 네트워크에 연결하기 전에 세심한 보안 검토가 있어야만 할 것이다.

2.2.2 신뢰성있는 호스트(Trusted Hosts)

Trusted Host 개념은 Berkeley 계열, 즉 BSD UNIX를 사용하고 있는 SUN VAX 등의 운영체제에서는 네트워킹 유틸리티의 기본 개념으로서, Remote Login, Remote Command Execution 등은 적절한 사용자가 이를 사용할 때 사용자 계정 및 패스워드 등을 요구하지 않게 되는데, 이는 편리함을 주지만 Internet Worm이 자신의 프로그램을 위해 이 개념을 악용한 것처럼 보안의 문제를 야기한다. 하지만 매우 편리한 개념이므로 여기에서는 적절한 설치구현을 통하여 보안성을 유지하는 방법을 보기로 한다.

먼저 시스템 관리자가 Trusted Hosts를 지정하는 방법으로서 hosts.equiv 화일이 있다. 사용자가 rlogin과 rsh 등을 수행할 때, 여기서 호스트를 체크한 후 사용자의 계정이 동일하면 패스워드 없이 액세스 가능하다. 동일한 기관이나, 로컬환경이 아니라면 그리고 개방된 Terminal Room 등이 액세스 가능한 호스트는 결코 신뢰해서는 안될 것이다. Yellow Page를 지원하는 SUN 시스템에서는 만약 hosts.equiv 화일이 단하나의 라인에 "+"를 자동적(Default) 값으로 가지고 있는데 모든 호스트 Trusted Host로 여기고 있다는 것이므로 이는 보안 문제를 야기하게 되므로, 적절하게 운영하려면 결코 "+"을 쓰면 안되는 것이다. 즉, "+"는 특정의 호스트에 대해서만 사용해야 할 것이다.

그리고 host.equiv와 유사한 개념으로서 .rhosts 화일이 있는데, 다만 적절한 host-user의 대응이 필요한 것으로 사용자는 자신의 HOME 디렉토리에 Trused Host를 생성할 수 있는 것이다. 이러한 방식은 관리자가 모르는 Trusted Host를 생성함으로서 심각한 보안문제를 제기할 수 있으므로, 관리자는 이를 허용하지 말아야 하므로 항상 사용자의 .rhosts를 모니터 해야 하고 다만 관리자(root)는 네트워크를 통한 백업 등을 위해서라도 이를 적절히 가진다.

2.2.3 보안성있는 터미널

SUN 시스템을 비롯한 새로운 버전의 UNIX는 보안성있는 터미널을 제공하고 있다. 즉 보안이 지정된 터미널에서는 root 패스워드를 알고 있다고 하여도 액세스 할 수 있도록 하는 기능으로서, /etc/ttytab이 이러한 기능을 줄 수 있도록 되어있다.

```
# @(#)ttytab 1.4 88/02/07 SMI
# name getty                              type          status      comments
console "/usr/etc/getty std.9600" sun          off secure
ttya "/usr/etc/getty std.9600" unknown         off secure
ttyb "/usr/etc/getty std.9600" unknown         off secure
ttyh0 none                              network       off secure
```

마지막의 "secure"는 보안이 제공된다는 의미이므로 만약 이런 구성을 지우고 싶을 때는 "secure"를 지우고,

```
# kill-HUP 1
```

을 하게되면, init 프로세스가 ttytab을 다시 읽게 된다. 보안터미널 개념은 가상터미널(Pseudo Terminal)도 네트워크로부터 액세스를 막기위해 적용된다. 하지만 가장 보안이 잘된 경우는 secure를 콘솔도 포함, 지우고 관리자도 su를 이용하여 액세스하도록 하는 것이다.

2.2.4 네트워크 화일 시스템 (Network File System, NFS)

SUN 시스템의 MFS는 특히 디스크없는 워크스테이션들이 서버의 디스크를 공유할 수 있도록 한 유용한 유털리티 이지만, 보안기능이 약하여 Internet의 어느 시스템도 허락없이 액세스 가능하기 때문에 보안의 헛점이 될 가능성이 있다. 하지만 SUNOS4.0 이상부터 공개키방식에 의한 암호화를 비롯 보다 보안성 있게 할 수 있는 방법이 있다.

/etc/exports 화일은 NFS의 구성상 가장 중요한 화일로서, 외부로 마운트되는 화일 시스템의 리스트를 열거한다. 즉,

```
/usr
/home
/var/spool/mail
#
/export/root/client1 -access=client1, root=client 1
/export/swap/client1-access=clinet1, root=client 1
```

에서 "root=keyword"는 그 화일시스템에 관리자가 액세스 가능하다는 것이며, 그리고 "access=keyword"는 ":"에 의해 구별되어 그 화일시스템이 마운트 될 수 있는 호스트의 리스트로서, 만약 "access=keyword"가 없다면 어떤 후스트도 마운트할 수 있어 보안에 문제가 되므로 관리를 잘해야 한다. 만약 몇개의 호스트만 있다면,

```
/usr -access=host1 : host2 : host3 : host4 :  host5
```

로 지정하면 된다. 이렇게 바뀐 exports 화일은,

```
# exportfs -a
```

통해 다시 시작한다.

Yellow Page에 의해 유지되는 네트워크 그룹을 정의하는 /etc/netgroup 화일은,

```
1.__Group        (Servera,,) (Clienta1,,) (Clienta2,,)
2.__Group        (Serverb,,) (Clientb1,,) (Clientb2,,)
Netadmin (Clienta1, kim,) (Clientb3, lee,)
Allgroup 1__Group 2__Group
```

과 같은데, 여기서 1__Group, 2__Group, Netadmin, Allgroup들이 네트워크 그룹이다. 이러한 네트워크 그룹들은(host, user, domain)에 의해 정의되며, 네트워크 그룹을 이용하여 NFS의 액세스를 제한할 수 있는데, 바꾼 /etc/exports를 보면,

```
/usr          -acces=1__Group
/home         -access=1__Group : 2__Group
/var/spool/mail -access=Allgroup
#
/export/root/client1-access=client1, root=client 1
/export/swap/clint1-access=client1, root=client 1
```

으로서, /usr 화일시스템은 1__Group에 있는 호스트에만 마운트되는 제한이 생겼다.

2.2.5 화일전송(File Transfer Protocol, FTP)

화일전송은 ftp, ftpd, tftp로 구현되어 있고, 구버젼들은 조금 에러가 있으므로 시스템 보안에 문제가 된다. 만약 1988년 12월 버젼이전의 BSD UNIX는 새로운 비젼을 구해야 한다. 화일전송에서 가장 유용한 기능은 "anonymous"로그인 기능이다. 이는 특정한 디렉토리에서만 액세스 가능하도록 한 개방된 소스 프로그램이나 정보를 배포하는데 이용된다. anonymous FTP를 구성하는 방법은,

1. 패스워드가 "*"인 "ftp" 계정을 만든다. HOME은 주로 /usr/ftp 이다.
2. 쓰기 기능을 없앤다.

```
# chown ftp~ftp
# chmod 555~ftp
```

3. ~ftp/bin 디렉토리를 만들고, ls를 복사해 둔다.

```
# mkdir~ftp/bin
# chown root~ftp/bin
# chmod 555~ftp/bin
# cp -p /bin/ls ~ftp/bin
# chmod 111 ~ftp/bin/ls
```

4. ~ftp/etc 디렉토리를 만들고, /etc/passwd, /etc/group을 복사하는데, 모든 패스워드는 "*"로 만들거나, "ftp" 계정만 둔다.

```
# mkdir ~ftp/bin
# chown root ~ftp/etc
# chmod 555 ~ftp/etc
# cp -p /etc/passwd/etc/group ~ftp/etc
# chmod 444 ~ftp/etc/passwd ~ftp/etc/group
```

5. ~ftp/pub 디렉토리를 만든다.

```
# mkdir ~ftp/pub
```

```
# chown ftp ~ftp/pub
# chmod 777 ~ftp/pub
```

으로서 이러한 anonymous FTP 기능은 각각의 네트워크마다 하나씩만 두어 모니터를 쉽게하는 것이 좋으며, ~ftp/pub 디렉토리를 쓰기 가능하게 만들어 두었을 경우에는 항상 체크하여 이상한 프로그램은 지우는 것이 좋다.

간단한 화일 전송프로그램인 Trivial FTP(TFTP)는 디스크 없는 워크스테이션들의 네트워크 부트(Boot) 기능으로 사용자 데이타그램(User Datagram)방식의 접속없는 프로토콜을 사용한다. 단순한 프로토콜이므로 시큐리티 문제를 가지고 있다.

```
% tftp
tftp>connect myhost
tftp>get/etc/motd tmp
Error code 1 : File not found
tftp>quit
#
```

만약 에러가 발생한다면, tftpd를 새버젼으로 교체해야 한다.

2.2.6 전자우편(Mail)

전자우편 시스템은 외부망과의 연결에 필수적인 유틸리티로서 BSD UNIX에는 우편의 배달과 수신을 담당하는 sendmail 프로그램이 있는데, 이도구버젼에는 보안문제를 가지고 있다. 이것은 Internet Worm에서 심각한 보안문제를 일으킨 바 있으므로, 최근의 버젼인 5.61로 교체해야 한다. sendmail의 설치시 고려해야 할 보안문제는 다음과 같다.

1. /etc/aliases나 /usr/ucb/aliases에서 "decode"를 제거한다.
2. 만약 프로그램에 메세지를 보내는 경우에는 shell 명령을 보내는 방법을 사용하지 않도록 한다.
3. sendmail.cf에서 "wizard" 패스워드를 사용하지 않는다.
4. sendmail에서 "debug" 명령을 사용하지 않는다.

이것은 다음을 참고.

```
garam% telnet localhost 25
Connected to localhost.
Escape character is '^]'.
220 garam Sendmail 4.0 ready at Sun, 16 Jun 91 14 : 09 : 22 KDT
debug
500 Command unrecognized
quit
221 garam closing connection
Connection closed by foreign host.
garam%
```

만약 "debug"에 "200 Debug set"으로 응답한다면, 새 버젼으로 교체해야 한다.

2.2.7 핑거(Finger)

finger 프로그램은 사용자의 정보를 보여주는 기능으로서 sendmail과 마찬가지로 Internet Worm에서 사용자 정보를 얻기 위하여 사용되었으므로, 새 버젼으로 교체해야 한다.

```
garam% finger chilm
Login name : chlim          In real life : Chaeho Lim
Directory : /staff/chlim    Shell : /bin/csh
On since Jun 16 10 : 53 : 51 on ttyp0 from 134.75.96.116
```

New mail received Sat Jun 15 14 : 08 : 16 1991 ;
unread since Sun Jun 16 10 : 54 : 02 1991
No Plan.
garam%

2.2.8 모뎀과 터미널 서버

모뎀이나 터미널 서버(Terminal Switch, Annex Box 등) 들은 보안문제를 항상 가지고 있다. 주요문제는 잘못된 구성에 기인하는 것으로서 여러가지를 지적할 수 있겠지만 다음을 고려할 수 있겠다.

1. 만약 사용자가 모뎀으로 Dial Up 해서 전화를 끊었을 때, 시스템은 그를 로그아웃시켜야 하는데, 그렇지 않을 경우 하드웨어 연결이나 Port의 kernel을 체크해야 한다.

2. 사용자가 로그아웃했을 때, 모뎀이 회선을 끊도록 해야 한다. 그렇지 못할 경우 하드웨어 연결을 체크해야 한다.

3. 터미널서버에서 시스템 연결이 끊어졌을 경우 시스템은 사용자를 로그아웃시킬 수 있어야 한다.

4. 만약 터미널서버가 모뎀에 연결된 사용자의 회선에 이상이 있을 경우, 서버는 시스템에 이 사실을 알릴 수 있어야 한다.

보통 이러한 장비들의 설치 매뉴얼을 조심해서 체크하도록 해야 하는데, 특히 "Carrier Detect", "Clear to Send", "Request to Send" 연결을 주시해야 한다.

2.2.9 방화벽개념(Firewalls)

새로운 보안의 개념으로 방화벽이 있다. 이름 그대로 이것은 외부망과 각자의 내부망 사이에 위치해서 외부망에 내부의 라우팅 정보를 보내지 않음으로서, 자신의 망이 외부에서 보이지 않도록 구성하는 것이다. 이를 위해 다음이 고려된다.

1. 방화벽 호스트는 라우팅 정보를 발행하지 않게 하여 외부망에서의 액세스는 모두 일단 방화벽 호스트에 로그인하여야 한다. 불편하긴 하여도 가장 보안성이 높은 방법이다.

2. 전자우편은 모두 방화벽이 재분배해야 하는데, 외부망에서 오는 전자우편은 각 사용자의 등록된 alias를 이용한다.

3. 방화벽 호스트는 NFS를 허용하지 않는다.

4. 방화벽 호스트에서의 passwd는 매우 강화되어 체크해야 한다.

5. 방화벽 호스트는 어떤 다른 호스트도 신뢰하지 않는다.

6. 방화벽 호스트에서는 요구된다면 Anonymous FTP나 유사한 서비스만을 제공하도록 한다.

2.3 화일시스템의 보안

2.3.1 개요

UNIX에서의 화일이나 디렉토리의 보안을 위해,

read 화일이나 디렉토리에 대한 읽기 동작
write 쓰기동작,(수정)
execute 수행동작,(찾기)

의 권한(Permission) 비트가 제공되는데, 각각의 권한비트에 대해 다른 기능이 제공되는 4번째의 권한비트가 또 제공된다. 이것은 아래와 같다.

setuid 사용자 권한에 세트되면, 사용자의 수행권한 뿐 아니라, 소유수행 권한을 가진다. 예를 들어, sendmail은 "root"로 setuid되어 있어 우편큐에 쓰기를 할 수 있으나 보통의 사용자는 안됨,

setgid 이것은 그룹권한에 세트되어 setuid와 같은 기능을 함,

sticky 이것은 모든 권한에 적용되며, 수행가능한 화일의 테스트 이미지에 어떤일을 하도록 운영체제에게 알린다. 오래된 UNIX에서 도입되었으나 현대는 쓰지 않음.

2.3.2 setuid 쉘스크립트(Shell Script)

setuid나 setgid를 위해 Shell Script가 많이 있으며, 보안장치가 있다고는 하고 있으나, 모든 보안문제를 모두 해결하지는 못하므로 UNIX에서는 보안을 위해서라면 이것을 허용해서는 안된다.

2.3.3 디렉토리의 Sticky 비트

새로운 버전의 UNIX에서는 또다른 개념의 Sticky 비트를 디렉토리에 이용하고 있는데, 사용자는 디렉토리내의 다른 사용자의 화일 디렉토리를 지우거나 고칠 수 없도록 하는 기능이다. /tmp 디렉토리를 생각하면 된다. 이를 위해서는,

chmod o+t directory

를 사용하면 된다.

2.3.4 디렉토리의 setgid 비트

이것은 두가지의 규칙이 SUNOS에서는 적용되는데,

1. System V 메카니즘으로서, 사용자의 주요 그룹 id가 생성하는 모든 화일에 적용되는 것,
2. Berkeley 메카니즘으로서, 화일의 그룹 id는 해당하는 디렉토리의 그룹 id에 적용된는 것,

으로서, setgid 비트가 디렉토리에 적용되면 Berkeley 메카니즘이 적용되고 그렇지 않으면 System V 메카니즘이 적용된다. 보통 Berkeley 메카니즘을 다음과 같이 적용하여, 해당 그룹의 가입자가 함께 쓰는 디렉토리를 생성한다.

chmod g+s directory

2.3.5 umask 값

만약 에디터나 컴파일러 등을 통해 화일을 생성할 때의 권한비트를 조정하는 것이 umask를 이용하는 것이다. 보통 시스템에서는 umask를 022로 하여 그룹과 모든 사용자로의 권한을 막는 것이다. 각 사용자는 시스템의 umask를 자신의 cshrc나 .profile에 이것을 다르게 지정할 수가 있다. 하지만 "root"는 항상 022로 해두어 돌발적인 보안사고에 대비해야만 한다.

2.3.6 화일의 암호화

UNIX의 crypt는 이미 세계 제 2차 대전에서 깨졌던 암호화 알고리즘을 여전히 사용하고 있으며, 이의 해독 프로그램도 이미 돌아다니고 있는 실정인데, 새로운 알고리즘인 DES도 벌써 그 보안성에 의문이 제기되고 있는 실정이다. 가장 보안성이 높은 것은 만약 암호화 할 정도의 중요한 화일이라면, UNIX나 개인용 컴퓨터와 같은 곳에서는 보관을 하지 않는 것이다. UNIX의 passwd는 crypt를 사용하지 않고 단방향의 DES를 이용하고 있으므로 사용자의 로그인시, 복호화하지 않고, 다시 암호화하여 저장되어있는 패스워드와 비교한다.

2.3.7 디바이스(Devices)

디바이스의 보안은 매우 중요하다. /dev 디렉토리에 있는 모든 종류의 디바이스들은 여러 프로그램들이 액세스하게 되므로 만약 적절하게 보호되지 않는다면 시스템 공격자에게 좋은 표적이 될 것이다. 몇가지만 보기로 하자.

1. /dev/kmem, /dev/mem, /dev/drum 등은 결코 다른 사용자에게 읽혀질 수 있어서는 안된다. 만약 "kmem" 그룹이 지원된다면, 열거한 화일들은 "root"나, "kmem" 그룹에 의해 소유되고 모드 640이 되어야하며, 만약, "kmem" 그룹이 지원되지 않는다면, "root" 소유에 600이 되어야 한다.
2. 디스크 디바이스인 /dev/sd0a, /dev/xy1b, /dev/rst0 등은 사용자, "root", 그룹 "operator"에 속하고 모드 640으로 지정되어야 한다.
3. 그리고는 terminal만 제외하고는 "root"가 소유할 수 있도록 해야 하며 Terminal은 로그인한 사용자의 소유이다가 로그아웃과 동시에 "root"로 자동적으로 반환된다.

3. UNIX 보안 모니터링 방법

3.1 사용자 계정의 모니터링

3.1.1 lastlog 화일

/usr/adm/lastlog는 각 사용자의 최근 시스템로그인 시간을 가지고 있는데, 사용자는 로그인 할 때마다,

와 같은 메세지를 보게되는데, 이것은 lastlog 화일에 저장되고, finger 프로그램도 이것을 사용한다. 각 사용자는 로그인할 때마다 시간을 체크하여 이상이 있을 경우 관리자에게 보고해야 한다.

3.1.2 utmp 및 wtmp 화일

/etc/utmp는 현재 로그인된 사용자를 보여주고 who 명령어로 볼 수 있다.

```
% who
root console Jun 14 17 : 10
chlim ttyp0 Jun 16 23 : 24(garam 2. seri. re. kr)
telnet ttyp1 Jun 16 22 : 51(adam. kaist. ac. kr)
root ttyp6 Jun 15 10 : 25(sorak. kaist. ac. kr)
taeha ttyp9 Jun 15 10 : 42(consmos. kaist. ac. kr)
%
```

그리고 /usr/adm/wtmp 각 사용자의 로그인 시간과 로그아웃 시간을 기록해 두고 있는데, last 명령어를 사용하여 볼 수 있다.

```
garam% last
ywcho ttyp0 cray2s. seri. re. k Tue Jun 4 09 : 34－09 : 34 (00 : 00)
sdseo ttyp4 sunc50. seri. re. k Tue Jun 4 09 : 22－09 : 47 (00 : 25)
jwpark ttyp3 ns. seri. re. kr Tue Jun 4 09 : 12－09 : 31 (00 : 19)
chlim ttyp1 134. 75. 96. 116 Tue Jun 4 09 : 01－crash (12 : 51)
ohbyeon ttyp2 134. 75. 100. 95 Tue Jun 4 09 : 00－09 : 40 (00 : 40)
microgen ttyp0 pgd1. kaist. ac. kr Tue Jun 4 08 : 25－09 : 28 (01 : 02)
wtmp begins Tue Jun 4 07 : 59
garam%
```

3.1.3 acct 화일

/usr/adm/acct는 시스템에서 수행된 명령어를 기록해 두는데, kernel이 컴파일 될 때, SYSACCT 옵션을 가지고 있어야 한다. 이 화일은 lastcomm 명령어로 볼 수 있다.

```
garam% lastcomm
cpp        root __ 0. 05 secs Tue Jun 4 00 : 00
sed        root __ 0. 09 secs Tue Jun 4 00 : 00
grep       root __ 0. 06 secs Tue Jun 4 00 : 00
sh    S    root __ 0. 08 secs Tue Jun 4 00 : 00
sh    F    root __ 0. 02 secs Tue Jun 4 00 : 00
ifconfig S root __ 0. 02 secs Tue Jun 4 00 : 00
cat        root __ 0. 05 secs Tue Jun 4 00 : 00
mkACCT S root __ 277. 06 secs Mon Jun 3 23 : 35
```

3.2 네트워크의 모니터링

3.2.1 syslog 기능

syslog 기능은 명령의 에러나 로그인 등의 정보를 콘솔에 디스플레이 하면서, 로그인 화일을 만들어 주는데, /usr/adm/messages 화일에 기록한다. 이를 보면,

```
Dec 27 10 : 31 : 54 garam login : ROOT LOGIN ttyp0 FROM pigeon.seri.re.k
Dec 27 10 : 38 : 07 garam named[302] : restarted
Dec 28 09 : 59 : 35 garam login : ROOT LOGIN ttyp4 FROM gaya.seri.re.kr
Dec 28 10 : 08 : 33 garam su : BAD SU leebd on/dev/ttyd1
Dec 28 10 : 08 : 37 garam su : leebd on /dev/ttyd1
Dec 28 10 : 30 : 20 garam vmunix : BAD TRAP
Jan 4 13 : 40 : 35 garam login : ROOT LOGIN ttyp6
```

여기서 흥미로운 것은 LOGIN과 su로서 직접 root로 로그인할 경우 추적할 수 없으므로 su를 사용하도록 해야하며, 만약 로그인이 3번 이상 실패하면 로그인이 거절되고 그의 기록이 남게된다.

3.3 화일시스템의 모니터링

3.3.1 find 명령어

find 명령을 잘 이용하면 화일 시스템에서 보안 문제가 되는 화일들을 모니터 할 수 있다. 먼저 허가되지 않은 setuid, setgid 프로그램을 찾는 간단한 방법을 보기로 하는데, setuid "root" 프로그램은 공격자가 주로 이용하므로 심각한 보안문제를 가지고 있다.

```
# find/-type f -a\( -perm -4000 -o -perm  -2000\) -print
```

에서 각각의 옵션들을 설명하자면,

/	찾아야할 디렉토리,
-type f	보통화일(f)만을 찾음,
-a	그리고(and),
\(…)	… 옵션들의 그룹화,
-perm -4000	4000비트(set user id) 권한을 찾음,
-o	혹은(or),
-perm -2000	2000비트(set group id) 권한을 찾음,
-perm	화면에 디스플레이,

으로서 이것을 수행하는데는 한시간 이상 걸릴수도 있다. 그리고 결과 프로그램이 특히 /bin, /etc, /usr/bin, /usr/ucb, /usr/etc에 있는 것을 주의해야 한다. 단/usr/etc/restore는 setuid 비트가 세트되어 있는데, 이는

```
# chmod u-s/usr/etc/restore
```

를 통해 지워야 한다.

그리고, 모두 쓰기 가능한 화일을 찾으려면 다음을 쓴다.

find/ -perm -2 -print

또한 계정에 없는 소유자, 그룹명 없는 그룹의 화일을 찾기 위해서는,

find/home -name .rhost-print

를 쓴다.

사용자가 임의로 작성해둔 .rhost 화일은,

find/home -name .rhost -print

로 찾는데 이때, /home은 화일 시스템의 홈이다.

3.3.2 체크리스트(Checklists)

Checklists는 시스템의 디렉토리에 어떤 인가되지 않은 변화가 없었는지 체크하는 도구로서 공개된 프로그램들이 많이 있지만 여기서는 ls와 diff를 이용한 간단한 방법을 보기로 한다.

ls -aslgR/bin/etc/usr>MasterCheckList

여기서 나중에 똑같은 방법으로 CurrentCheckList 화일을 만들어,

diff MasterCheckList CurrentCheckList

로 간단하게 시스템 디렉토리의 변화를 체크할 수 있다.

3.3.3 백업(Back up)

어떤 백업이 가장 좋다고는 아무도 주장할 수 없지만, 적어도 한달에 한번 레벨 "0")Full) 백업과 2주일에 한번의 부분 백업을 권장한다. 그리고 백업을 위해서는 tar나, cpio 보다 "dump"를 권장하는데 이는 이것이 보다 정확한 재구성이 가능하기 때문이다.

3.4 시스템의 모니터링

ps 명령은 시스템의 현재 프로세스들의 현황들을 보여주는 기능으로서, 여기 그 많은 옵션들을 나열할 수는 없고 단지 SUNOS4.0 이상에서 기대해야할 것은,

swapper, pagedaemon, 가상메모리 관리를 위한 시스템 프로그램,

/sbin/init, 터미널로그인을 비롯한 많은 업무를 수행,

portmap, ypbind, ypserv, Yellow Page의 기능,

biod, nfsd, rpc.mountd, rpc.quotad, rpc.lockd, NFS(Client는 nfsd 없음),

rarpd, rpc.bootparamd, 디스크 없는 client를 위한 기능,

들이다.

그밖에 who, w, ls 명령들을 이용 시스템을 모니터할 수 있다.

4. 보안관련 프로그램

4.1 새버젼의 프로그램을…

UNIX 시스템은 끊임없이 에러를 수정하고 새로운 기능들을 추가하여, 매우 빠른 속도로 변하고 있으므로 항상 새로운 버젼의 시스템을 유지하도록 해야 할 것이다. 먼저 SUN 소프트웨의 새버젼은 anonymous FTP를 이용하여 가져올 수 있다.

```
% ftp ftp.uu.net
connected to uunet.UU.NET
220 uunet FTP server(Version 5.93 Tue Mar  20 11 : 01 : 52 EST 1991) ready.
Name(ftp.uu.net : chlim) : anonymous
```

331 Guest login ok, send ident as password.
password : chlim@garam.seri.re.kr
230 Guest login ok, access restrictions apply.
ftp>cd sun-fixes
250 CWD command successful.
ftp>ls

여기서 README를 가져와서 읽어보면 디렉토리의 내용들과 기타정보들을 알 수 있다.

Berkeley UNIX의 새버젼은 ucbarpa.berkeley.edu의 4.3/ucb-fixes 디렉토리에서 anonymous FTP 하면 된다.

기타 유용한 UNIX에서의 프로그램들은 wsmr-simtel20.army.mil에서 많은 소스프로그램들을 찾아볼 수 있고 기타 anonymous FTP 호스트리스트를 참고하기 바란다.

4.2 유용한 보안 패키지

보안에 관련한 유용한 소스프로그램들을 많이 찾아 볼 수 있겠지만, 여기서는 몇가지만 열거하기로 하는데, 먼저 텍사스 Austin 대학의 Clyde Hoover에 의해 개발된 npasswd는 UNIX passwd를 대체하기 위해 만든 프로그램으로서, 지원기능은,

1. 최소한의 패스워드 길이를 조정할 수 있다.
2. 사용자로 하여금 대소문자, 숫자, 마침점 등을 강요가능하다.
3. 단순한 패스워드를 체크해낼 수 있다.
4. 호스트 이름, 호스트 정보 등을 체크할 수 있다.
5. 로그인 이름, 성명 등을 체크할 수 있다.
6. 시스템 사전을 비롯, 여러 사전의 단어를 체크할 수 있다.

으로서, emax.utexas.edu에서 anonymous FTP 할 수 있다.

그리고 다른 유용한 것으로 COPS가 있는데 시스템 관리자가 여러가지 보안문제를 체크할 수 있도록 한 %스크립트와 C로 구성되고 UNIX에는 쉽게 구성할 수 있다. 제공하는 기능들을 보자면,

1. /dev/kmem과 다른 디바이스 화일의 읽기/쓰기를 체크,
2. 여러 중요화일의 잘못된 모드를 체크,
3. 단순 패스워드를 체크,
4. passwd 화일의 잘못을 체크,
5. group 화일의 잘못을 체크,
6. 모든 사용자의 cshrc, .profile, .login과 .rhost 화일 체크.
7. /etc/rc와 cron 화일을 체크,
8. NFS의 외부 마운트를 위한 "root"의 경로 체크,
9. 주어진 사용자를 체크하는 expert 시스템 기능,
10. setuid 상태의 변화를 체크,

으로서 이것도 ftp.uu.net의 comp.sources.unix 아카이브나, wsmr-simtel20.army.mil에서 anonymous FTP 할 수 있다.

Kerberos는 MIT의 Athena 프로젝트에서 개발한 인증(Authentication) 시스템으로서, Kerberos는 사용자의 로그인을 인증한 후, 그 사용자의 신원을 네트워크에 흩어져 있는 서버, 호스트에 증명해 준다. 이 Kerberos는 rlogin, mail, NFS 등에 다양하게 보안 기능을 제공하고 있지만 이 Kerberos를 설치하려면 많은 구성상의 수정이 불가피하여 어려운 점이 있다. 향후 Berkeley 4.4 버젼에 함께 이식할 계획이 있다.

4.3 SUN C2 기능

SUNOS4.0 이상은 National Computer Security

Center에서 정의하고 있는 C2 수준의 보안 보류를 만족하고 있는데, 시스템 배포 테잎의 옵션에 따라 설치할 수 있다. 이 보안 기능들은,

1. Audit Trail,
2. Shadow Password,
3. DES Encryption,
4. Secure NFS

등이라고 하겠다.

5. 관련 사항

미국의 Internet 환경에서는 보안 문제를 위해 여러가지 그룹과 정보교환 기능들을 가지고 있다. 그 기능과 주제별로 살펴보면,

1. 컴퓨터 비상응답팀(Computer Emergency Response Team, CERT) CERT는 1988년 미국방성 첨단프로젝트 관리국(Defence Advanced Research Projects Agency, DARPA)가 지원하여 카네기멜런 대학의 소프트웨어 연구소(Software Engineering Institute)가 운영하고 있는 보안문제를 집중연구하고 Internet에 서비스하는 역할을 담당한다. 24시간 Hot-line을 운영하고 있으며, Mailing List도 운영하고 있으므로 누구나 가입할 수 있다.

2. DDN 관리 게시판(Bulletine)

Defence Data Network(DDN) 관리게시판 DDN의 정책, 절차, 기타정보들을 전자적으로 발송하는 기능이며, 특히 보안게시판(Security Bulletine)은 DDN Security Coordination Center(SCC)와 협조하에 DDN의 보안문제에 대한 정보를 제공하고 있다.

3. 보안관련 Mailing List

security-request@cpd.com,	시스템 관리자를 위한 보안정보
risks-request@csl.sri.com,	ACM Committe에서 관리
tcp-ip-request@nic.ddn.mil	TCP/IP 프로토콜 관련
sun-spots-request@rice.edu	SUN 시스템 하드웨어 관련
sun-nets-request@umiacs.umd.edu	NFS, Yellow Page, Name Server
sun-managers-request@eecs.nwu.edu	모든 SUN 시스템관리·정보

listserv%lehiibm 1.bitnet@mitvma.mit.edu VIRUS

6. 결 론

국외의 최근 자료와 현재 시스템 공학 연구소에서 추진하고 있는 연구를 참고로 미비하나마 기술보고 형식으로 UNIX 보안을 점검하여 보았다. 물론 이러한 노력도 보다 교묘하고 또 공격적인 해커들에게는 무용지물이 될지 모르겠지만, 이러한 작업들은 현재보다는 더욱 보안을 높혀주고, 또 해외망과의 적극적인 정보의 교류를 통해 지속적인 시스템 보안을 향상 시켜야 할 것이다.

국내에서도 UNIX 기종과 또 관련한 전산망을 확대 일로에 있는 상황이라고 볼 수 있는데, 특히 국내 연구전산망(Korea Research Environment Open Network, KREONet)과 하나(HANA), System Development(SDN), KREN 등이 이제는 각각 Internet, NSFNET, BITNET 등에 국제적인 연결이 이루어져 있으므로 해외로부터의 호기심어린, 혹은 악의적인 목적을 가지고 아직은 초보적인 수준이라고 볼 수 있는 국내망에 침투할 가능성이 매우 높아졌다고 본다.

벌써 연구전산망에서도 해외에서의 불법적인 액세스의 경험과 특히 국내의 해커들도 만만하지 않은 도전을 공공연하게 시도하고, 국내의 해커는 벌써 해외에도 연결을 호시탐탐 노리고 있다. 하나네트워크는 국내의 여러 네트워크와 연결되어서 특히 여러 보안문제가 발생하고 있는 것으로 발표되고

있다.

그러므로 특히 각 기관은 각자의 네트워크 시스템에 보다 세심한 보안에 신경을 쏟아야 할 것으로 보며, 본문의 방화벽 개념을 일부라도 도입한 게이트웨어/서버를 구성 유지해야 할 것이다. 뿐만 아니라 기관을 상호 연결하는 국내의 기간전산망을 비롯한 여러 전산망에서도 보안문제를 항상 염두에 두고 망을 구성해야 하리라고 본다.

끝으로 국내에서도 이러한 보안문제에 대한 협의회, 네트워크 토론 그룹, 나아가 보안 전문센터가 발족되어야 기술선도와 아울러 보다 원활한 협조체제를 이룰 수 있으리라고 판단한다.

참고 A. 추천도서

Improving The Security Of Your UNIX System
David A. Curry
SRI International, April 1990

UNIX System Administration Handbook
F. T. Grammp, R. H. Morris
AT&T Bell Lab. Technical Journal, 1984

Password Security : A Case History
Robert Morris, Ken Thompson
Communications of ACM, Nov. 1979

On The Security of UNIX
Dennis M. Richie
May 1975

The Cucko's Egg
Clifford Stoll
Doubleday, 1989

System and Network Administration
Sun Micro Systems
May 1988

Security Problems in the TCP/IP Protocol Suite
S. M. Bellovin
ACM Computer Communication Riview, April 1989

A Weakness in the 4.2 BSD UNIX TCP/IP Software
Rober T. Morris
AT&T Bell Lab. Computer Science Technical Report 117

Computer Virus and Related Threats : A Management Guide
John P. Wack and Lisa J. Carnahan
NIST Special Publication 500-166

참고 B. UNIX 보안 체크리스트

〈사용자계정 보안〉

패스워드 정책이 사용자에게 전달되었는가.
모든 패스워드는 적절한가.
모든 계정에 만기일이 적용되었는가.
사용자 없는 계정은 없는가.
모든 계정이 패스워드를 가지고 있는가. 혹은"*" 그룹계정은 없는가.
Yellow Page가 있다면 "+"는 적절한가.

〈네트워크 보안〉

host.equiv는 로컬호스트만 있는가."+"은 없는가.
사용자의 HOME 디렉토리에 .rhost 화일은 없는가.
단지 root만 .rhost를 가지고 있는가.
/etc/ttytab에는 console 만이 "secure"인가(서버에만 적용).
/etc/ttytab에는 어떤 터미널이 "secure" 되어있지는 않는가(Client만 적용).
NFS가 외부망에 개방되어 있지는 않은가.
ftpd가 새로운 버전인가.
aliases 화이리에 "decode"가 있지 않은가.
sendmail.cf에 "wizard"가 있지 않은가.
sendmail.cf에 "debug"가 있지 않은가.
fingerd가 새버젼인가.
모듈과 서버가 전화회선이 끊어질 경우 잘 처리하는가.

〈화일시스템 보안〉

setuid, setgid %스크립트는 없는가.
비인가된 setuid, setgid 프로그램을 체크하는가.
/usr/etc/restore의 setuid 비트가 제거되었는가.

외부망에서 쓰기 가능한 데렉토리가 sticky 비트를 가지고 있는가.
"root" 계정에 적절한 umask가 설정되었는가.
/dev 하의 디바이스 화일들의 모드가 적절한가.

백업

매달 "0" 수준의 dump를 실시하는가.
2주에 한번 부분 dump를 하는가.

□ 著者紹介

임 채 호(정회원)

1985年 弘益大學校 電算學科 卒業(學士)
1985年 韓國科學技術研究院 시스템공학센터 研究院
1989年 建國大學校 電子計算學科 大學院 卒業(碩士)
1991年 University of Maryland 電子計算學科, 訪問研究院
現在 韓國科學技術研究院
시스템공학 研究所 教育研究網 그룹 先任研究院

관심분야 : TCP/IP, OSI, OSI Security